Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 215 (2022) 483–487

Procedia Computer Science

www.elsevier.com/locate/procedia

4th International Conference on Innovative Data Communication Technology and Application

Cybersecurity vs. Information Security

Hamed Taherdoost [a,*]

[a] *Department of Arts, Communications and Social Sciences, University Canada West, Vancouver BC V6B 1V9, Canada*

Abstract

Protection of data assets is a hot trend topic that is attracting considerable interest worldwide. There are different concepts revolving security of data including cybersecurity and information security. Cybersecurity and information security terms are both related to the security of data aiming to defend data against different types of threats. Despite cybersecurity and information security are often used interchangeably, there are differences in each concept, and they should not be used interchangeably. Various definitions of cybersecurity and information security provided by scholars and standards are discussed in this article and differences are explained.

Keywords: Cybersecurity, Information Security, Security, Cyber Security.

1. Introduction

Technology brings along many advantages; however, it also invokes harassment and violence and causes embarrassment by motivating hackers to attack computer systems [1]. Documents to outline the strategy in cyberspace are officially published in over 50 nations [2]. A unified approach to define how the USA engages in cyber-related issues has been outlined and the United Kingdom introduced cyberspace as a major area of investment.

As reports share more news about cyber-attacks and the activity of hackers leading to significant failures for both businesses and individuals, a wider spectrum of stakeholders gets attracted to minimize the irreparable impacts of

* Corresponding author. Tel.: +1-236-889-5359.
E-mail address: hamed.taherdoost@gmail.com

10.1016/j.procs.2022.12.050

growing security risks. Hackers are likely to penetrate the computer of an ordinary citizen or access to accounts of a bank leading to serious risks for the board of directors as they are accountable for cyber risks [3].

The Internet and data volume has expanded over the years and cyber risks have grown accordingly threatening businesses that are reliant on data [4]. Cyber threat is a critical concern that jeopardizes information systems and their sustainability in the information ecosystem. A cyberattack puts information in a vulnerable state [5]. In recent years, the number of invaders to information systems is rapidly growing which is making the matter more dangerous [6].

It seems that there is no way to evade this trend in the age of data. However, a number of existing frameworks and standards have addressed the data security issues by focusing to minimize or eliminate them [5]. Reliance on standards and frameworks and following a range of security steps secures businesses and individuals from cyber risks to a great extent [7].

Thus, a new area of knowledge is developed to address security concerns as Cybersecurity and Information Security are commonly used terms today. These terms are commonly used interchangeably [3]. It is true that applying something to address cyber risks is rather than nothing; however, a better understanding in this area decreases the costs of data breaches to a great extent [8].

Cybersecurity and Information Security are both responsible to protect computer systems against cyber threats but what makes these two terms stand out differently?

2. Definitions of Cybersecurity and Information Security

To define Cybersecurity and Information Security, we have referred to ISO/IEC 27032:2012 and ISACA CSx Cybersecurity Fundamentals Study Guide as reputable sources in this area. Based on the ISO/IEC 27032:2012, Cybersecurity is defined as the "preservation of the confidentiality, integrity, and availability of information in Cyberspace". Also, the Merriam-Webster dictionary defines Cybersecurity as "measures taken to protect a computer or computer system against unauthorized access or attack". Information Security, on the other hand, is defined as the "preservation of the confidentiality, integrity, and availability of information". The main objective of Information Security is to ensure the continuity of business processes with the least damage and limit the negative impacts of incidents [9].

Other definitions of Cybersecurity and Information Security extracted from different references are presented in Table 1.

Table 1. Cybersecurity and Information Security Definitions

Information Security	Cybersecurity
Information security considers the security of computer systems to protect them against disclosure, subjective modification, unauthorized access, harassment, or destruction aiming to ensure integrity, confidentiality, and availability of information [10].	Cybersecurity considers the security of individuals and enterprises to protect them against security breaches, incidents, and intentional attacks on systems [10].
Information security includes protecting information against different threats aiming to minimize the risk of business activities, maximize return on investments, exploit business opportunities, and ensuring continuity of business. Information security considerations target integrity, confidentiality, and availability of information resources [1].	The scope of cybersecurity is extended to protect information and ICT involving maintaining integrity, confidentiality, and availability of information resources in cyberspace [1].
Information security considers integrity, confidentiality, and availability of information regardless of the type of data whether it is printable or electronic [11].	Cybersecurity includes the protection of tools, systems, processes, concepts, methods, and strategies aiming to protect properties in cyberspace against unauthorized access and loss of information leading to maintaining integrity, confidentiality, and availability of resources [11].
Information security is defined by the ISO/IEC 27002 (2005) international standard as ensuring integrity, confidentiality, and availability of different types of information whether it is electronic,	Cybersecurity is defined by the International Telecommunications Union (ITU) as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can

Information Security	Cybersecurity
soft copy, hard copy, delivered in conversation and films, or any other formats [12].	be used to protect the cyber environment and organization and user's assets" [12].
Technical and administrative measures that are taken to preserve the availability, confidentiality, and integrity of information are referred to as information security [13].	Cybersecurity refers to measures that are taken to provide friendly use of computer systems and deny unauthorized exploitation of information [13].
Information security refers to the availability, integrity, and confidentiality of information [3].	Cybersecurity refers to the protection of information integrity, confidentiality, and availability in Cyberspace [3].
Information security is defined as "the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information" [1].	Collection of policies, tools, guidelines, concepts, approaches, measures, technologies, best practices, and training that are used to preserve organizational cyber assets and users are recognized as cybersecurity [1].
Employment of logical and physical access controls to ensure the security of data and prevent unauthorized access to data, data loss, data misuse, damage, disclosure, or destruction of data [14].	The collection of processes, tools, structures and resources that are employed to protect systems in cyber space are recognized as cybersecurity [14].

Thus, it can be concluded that although Cybersecurity and Information Security are so closely linked to each other and overlap in some aspects, the main difference is related to information. Information Security is concentrated to protect information everywhere, whereas Cybersecurity is specifically focused on information in cyberspace.

Based on the ISACA CSx Cybersecurity Fundamentals Study Guide, cybersecurity is recognized as a part of information security that aims to protect digital assets and Information Security targets information whether it is in digital or physical space [3]. As cyberspace is growing rapidly, both information security and Cybersecurity need to be continuously evaluated and innovated to get updated with the most recent modifications.

3. The Difference Between Cybersecurity and Information Security

Considering definitions provided by these basic sources, it can be concluded that Information Security fully includes Cybersecurity as one of its components. Cyber Security, on the other hand, is responsible to ensure the security of information against cyber threats and cyber-attacks while it is processed, stored, or transported. Access Controls, Procedural Controls, Compliance Controls, and Technical Controls are examples of Information Security, whereas Application Security, Network Security, Cloud Security, and Critical Infrastructure are examples of Cybersecurity [15].

An example to compare Cybersecurity and Information Security is when sensitive information is left on the desk of an employee and copied by a customer aiming to sell it to an unauthorized party. This is a case of an Information Security breach since Cyberspace is not involved in the process [16]. However, if this sensitive information was shared on social media by the employee hurting the reputation of the company, it was considered a breach in Cybersecurity as well as Information Security. Thus, Cybersecurity incidents can be generalized to information security leading to breaches in confidentiality, integrity, or availability of information and exposing an organization to the threat of information loss [5]. The difference between Cybersecurity and Information Security is represented in Figure 1.

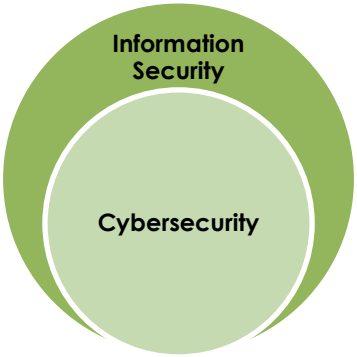

Fig 1. Difference between Cybersecurity and Information Security

4. Cybersecurity and Information Security from Different Aspects

Considering the differences between Cybersecurity and Information Security from different aspects, Cybersecurity protects cyberspace from cyber-attacks while Information Security considers protecting information from any form of threat regardless of being digital or physical. Thus, the scope of Cybersecurity is limited to cyberspace and Information Security deals with data protection in a wider realm [17]. In terms of threats, Cybersecurity provides protection against dangers in the digital environment while Information Security deals with threats that endanger information regardless of their type [18]. Attacks that endanger information in cyberspace include cyber frauds, cybercrime, and law enforcement [15]; however, any type of unauthorized access to information, disruption, or information disclosure is considered as an attack that should be addressed through Information Security [6].

Besides, professional standards are established to protect information from threats in cyber reals such as personal information on social media [19]; however, Information security professional standards consider the security of information assets to ensure information confidentiality, availability, and integrity.

5. Limitation and Future Directions

Existing cyber security and information security models are commonly based on the current status of data security and cyberspace; however, cyberspace is constantly growing. Thus, studies and models should be developed accordingly. Besides, this study is based on conceptual knowledge in this area and it does not cover any real case about the implementation of cyber security and information security in a case organization. Thus, it is recommended to conduct a study comparing the results of employing both information security and cyber security models in a case business for future directions.

6. Conclusion

Information has become of paramount importance to help organizations in achieving their business objectives and providing online services in the information-centric society. Despite the constructive role of information in the success of an organization, it is also likely to damage the reputation of the company and lead to significant failures if not protected. Besides, most businesses rely on cyberspace to manage their business processes, transfer information and deliver services. The more organizations are dependent on the Internet to offer services, cyber risks arise, and the necessity to get protected against cyber risks increases as well. Thus, Information Security and Cybersecurity terms are developed to address issues related to the security of information in an online or offline environment. Understanding Information Security and Cybersecurity and how they are different from each other better equip businesses to get protected against threats and risks of information loss.

References

[1] Reid, R., & van Niekerk, J. (2014). From Information Security to Cyber Security Cultures Organizations to Societies.
[2] Kovács, L. (2018). National Cyber Security as the Cornerstone of National Security. *Land Forces Academy Review*, 23, 11.120-3 . doi:10.2478/raft-2018-0013
[3] Solms, B., & Solms, R. (2018). Cyber security and information security – what goes where? *Information and Computer Security*, 26, 00-00. doi:10.1108/ICS-04-2017-0025
[4] Petratos, P. N. (2021). Misinformation, disinformation, and fake news: Cyber risks to business. *Business Horizons*, 64(6), 763-774.
[5] Smys, S., & Haoxiang, W. (2021). Data elimination on repetition using a blockchain based cyber threat intelligence. *IRO Journal on Sustainable Wireless Systems*, 2(4), 149-154.
[6] Karunakaran, P. (2020). Deep learning approach to DGA classification for effective cyber security. *Journal of Ubiquitous Computing and Communication Technologies (UCCT),* 2(04), 203-213.
[7] Goutam, R. K. (2021). *Cybersecurity Fundamentals: Understand the Role of Cybersecurity, Its Importance and Modern Techniques Used* by Cybersecurity Professionals (English Edition). BPB Publications.
[8] Taherdoost, H., Namayandeh, M., & Jalaliyoon, N. (2011). Information security and ethics in educational context: Propose a conceptual framework to examine their impact. *International Journal of Computer Science and Information Security*, 9(1), 134-138.
[9] Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information Security and Cybersecurity Management: A Case Study with SMEs in Portugl .*Journal of Cybersecurity and Privacy*, 1, 219-238. doi:10.3390/jcp1020012.
[10] G. Wang, & Wendy. (2019). Measuring information security and cybersecurity on private cloud computing. *Journal of Theoretical and Applied Information Technology*, 96(1), 156-168 .
[11] Andronache, A., & Althonayan, A. (2018). Shifting From Information Security Towards A Cybersecurity Paradigm.
[12] Santos, O. (2020). Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide (Certification Guide): Cisco Press.
[13] Maurer, T., & Morgus, R. (2014). Compilation of Existing Cybersecurity and Information Security Related Definitions.
[14] Collard, G., Ducroquet, S., Disson, E., & Talens, G. (2017). A definition of Information Security Classification in cybersecurity context. 11th International Conference on Research Challenges in Information Science (RCIS), Brighton, UK.
[15] Taherdoost, H., Chaeikar, S., Jafari, M., & Shojae Chaei Kar, N. (2013). Definitions and criteria of CIA security triangle in electronic voting system. *International Journal of Advanced Computer Science and Information Technology,* 1(1), 14-24.
[16] Taherdoost, H., Sahibuddin, S., & Jalaliyoon, N. (2015). How security issues can influence on usage of electronic services. *Advances in Information Science and Computer Engineering*, 310-316.
[17] Rabii, A., Assoul, S., Touhami, K. O., & Roudies, O. (2020). Information and cyber security maturity models: a systematic literature review. *Information & Computer Security*. 28(4), 627-644.
[18] Taherdoost, H., Sahibuddin, S., & Jalaliyoon, N. (2014). Evaluation of Security Factors Effecting on Web-Based Service Adoption. Recent *Advances in Telecommunications, Informatics and Educational Technologies*, 117-123.
[19] Jung, K. (2021). Extreme data breach losses: An alternative approach to estimating probable maximum loss for data breach risk. *North American Actuarial Journal*, 25(4), 580-603.